MIT Technology Review Subscribe

COMPUTING

How a Russian cyberwar in Ukraine could ripple out globally

Soldiers and tanks may care about national borders. Cyber doesn't.

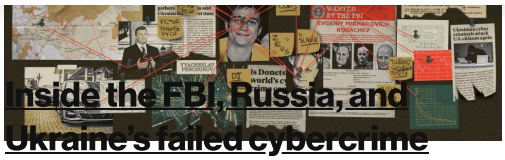
By Patrick Howell O'Neill

January 21, 2022

AP PHOTO

Related Story

Russia has sent more than 100,000 soldiers to the nation's border with Ukraine, threatening a war unlike



Inside the FBI, Russia, and Ukraine's failed cybercrime investigation

Russia and Ukraine promised to cooperate and help catch the world's most successful hackers. But things didn't quite go to plan.

yet, cyber operations are already underway.

Last week, hackers defaced dozens of government websites in Ukraine, a technically simple but attention-grabbing act that generated global headlines. More quietly, they also placed destructive malware inside Ukrainian government agencies, an operation first discovered by researchers at Microsoft. It's not clear yet who is responsible, but Russia is the leading suspect.

But while Ukraine continues to feel the brunt of Russia's attacks, government and cybersecurity experts are worried that these hacking offensives could spill out globally, threatening Europe, the United States, and beyond.

On January 18, the US Cybersecurity and Infrastructure Security Agency (CISA) warned critical infrastructure operators to take "urgent, near-term steps" against cyber threats, citing the recent attacks against Ukraine as a reason to be on alert for possible threats to US assets. The agency also pointed to two cyberattacks from 2017, NotPetya and WannaCry, which both spiraled out of control from their initial targets, spread rapidly around the internet, and impacted the entire world at a cost of billions of dollars. The parallels are clear: NotPetya was a Russian cyberattack targeting Ukraine during a time of high tensions.

"Aggressive cyber operations are tools that can be used before bullets and missiles fly," says John Hultquist, head of intelligence for the cybersecurity firm Mandiant. "For that exact reason, it's a tool that can be used against the United States and allies as the situation further deteriorates. Especially if the US and its allies take a more aggressive stance against Russia."

cyberattacks against Ukraine with its own cyber capabilities, further raising the specter of conflict spreading.

“My guess is he will move in,” Biden said when asked if he thought Russia’s President Vladimir Putin would invade Ukraine.

Related Story

The $1 billion Russian cyber company that the US says hacks for Moscow

Washington has sanctioned Russian cybersecurity firm Positive Technologies. US intelligence reports claim it provides hacking tools and runs operations for the Kremlin.

Unintentional consequences?

The knock-on effects for the rest of the world might not be limited to intentional reprisals by Russian operatives. Unlike old-fashioned war, cyberwar is not confined by borders and can more easily spiral out of control.

Ukraine has been on the receiving end of aggressive Russian cyber operations for the last decade and has suffered invasion and military intervention from Moscow since 2014. In 2015 and 2016, Russian hackers attacked Ukraine’s power grid and turned out the lights in the capital city of Kyiv— unparalleled acts that haven't been carried out anywhere else before or since.

The 2017 NotPetya cyberattack, once again ordered by Moscow, was directed initially at Ukrainian private companies before it spilled over and destroyed systems around the world.

NotPetya masqueraded as ransomware, but in fact it was a purely destructive and highly viral piece of code. The destructive malware seen in Ukraine last week, now known as WhisperGate, also pretended to be ransomware while aiming to destroy key data that renders machines

notable differences. For one, WhisperGate is less sophisticated and is not designed to spread rapidly in the same way. Russia has denied involvement, and no definitive link points to Moscow.

NotPetya incapacitated shipping ports and left several giant multinational corporations and government agencies unable to function. Almost anyone who did business with Ukraine was affected because the Russians secretly poisoned software used by everyone who pays taxes or does business in the country.

The White House said the attack caused more than $10 billion in global damage and deemed it “the most destructive and costly cyberattack in history.”

Since 2017, there has been ongoing debate about whether the international victims were merely unintentional collateral damage or whether the attack targeted companies doing business with Russia’s enemies. What is clear is that it can happen again.

Accident or not, Hultquist anticipates that we will see cyber operations from Russia’s military intelligence agency GRU, the organization behind many of the most aggressive hacks of all time, both inside and outside Ukraine. The GRU’s most notorious hacking group, dubbed Sandworm by experts, is responsible for a long list of greatest hits including the 2015 Ukrainian power grid hack, the 2017 NotPetya hacks, interference in US and French elections, and the Olympics opening ceremony hack in the wake of a Russian doping controversy that left the country excluded from the games.

Hultquist is also looking out for another group, known to experts as Berserk Bear, that originates from the Russian intelligence agency FSB. In 2020, US officials warned of the threat the group poses to government networks. The German government said the same group had achieved

"These guys have been going after this critical infrastructure for a long, a long time now, almost a decade," says Hultquist. "Even though we've caught them on many occasions, it's reasonable to assume that they still have access in certain areas."

Related Story

How Russian hackers infiltrated the US government for months without being spotted

And why it could take months more to discover how many other governments and companies have been breached.

A sophisticated toolbox

There is serious debate about the calculus inside Russia and what kind of aggression Moscow would want to undertake outside of Ukraine.

"I think it's pretty likely that the Russians will not target our own systems, our own critical infrastructure," said Dmitri Alperovitch, a longtime expert on Russian cyber activity and founder of the Silverado Policy Accelerator in Washington. "The last thing they'll want to do is escalate a

No one fully understands what goes into Moscow's math in this fast-moving situation. American leadership now predicts that Russia will invade Ukraine. But Russia has demonstrated repeatedly that, when it comes to cyber, they have a large and varied toolbox. Sometimes they use it for something as relatively simple but effective as a disinformation campaign, intended to destabilize or divide adversaries. They're also capable of developing and deploying some of the most complex and aggressive cyber operations in the world.

In 2014, as Ukraine plunged into another crisis and Russia invaded Crimea, Russian hackers secretly recorded the call of a US diplomat frustrated with European inaction who said "Fuck the EU" to a colleague. They leaked the call online in an attempt to sow chaos in the West's alliances as a prelude to intensifying information operations by Russia.

Leaks and disinformation have continued to be important tools for Moscow. US and European elections have been plagued repeatedly by cyber-enabled disinformation at Russia's direction. At a moment of more fragile alliances and complicated political environments in Europe and the United States, Putin can achieve important goals by shaping public conversation and perception as war in Europe looms.

"These cyber incidents can be nonviolent, they are reversible, and most of the consequences are in perception," says Hultquist. "They corrode institutions, they make us look insecure, they make governments look weak. They often don't rise to the level that would provoke an actual physical, military response. I believe these capabilities are on the table."

by Patrick Howell O'Neill

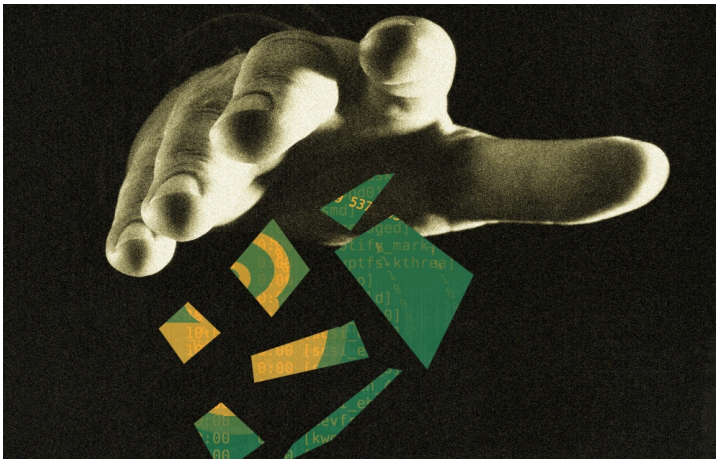
DEEP DIVE

COMPUTING

The code must go on: An Afghan coding bootcamp becomes a lifeline under Taliban rule

In Afghanistan, tech entrepreneurship was once promoted as an element of peace-building. Now, young coders wonder whether to stay or go.

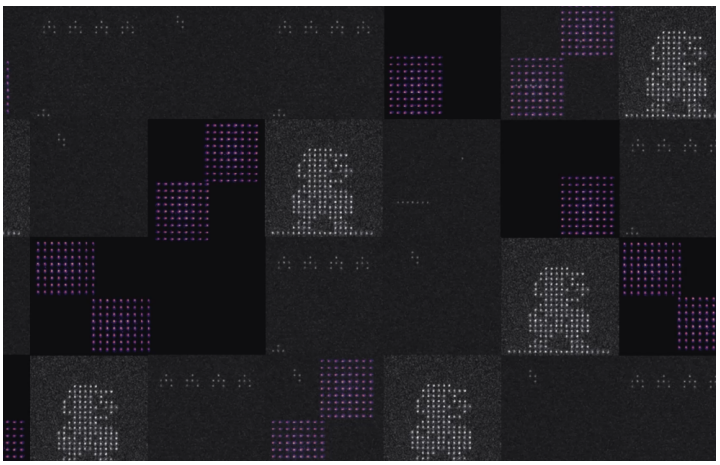
By Eileen Guo



fix it?

Volunteer-run projects like Log4J keep the internet running. The result is unsustainable burnout, and a national security risk when they go wrong.

By Patrick Howell O'Neill



This new startup has built a record-breaking 256-qubit quantum computer

QuEra Computing, launched by physicists at Harvard and MIT, is trying a different quantum approach to tackle impossibly hard computational tasks.

By Siobhan Roberts

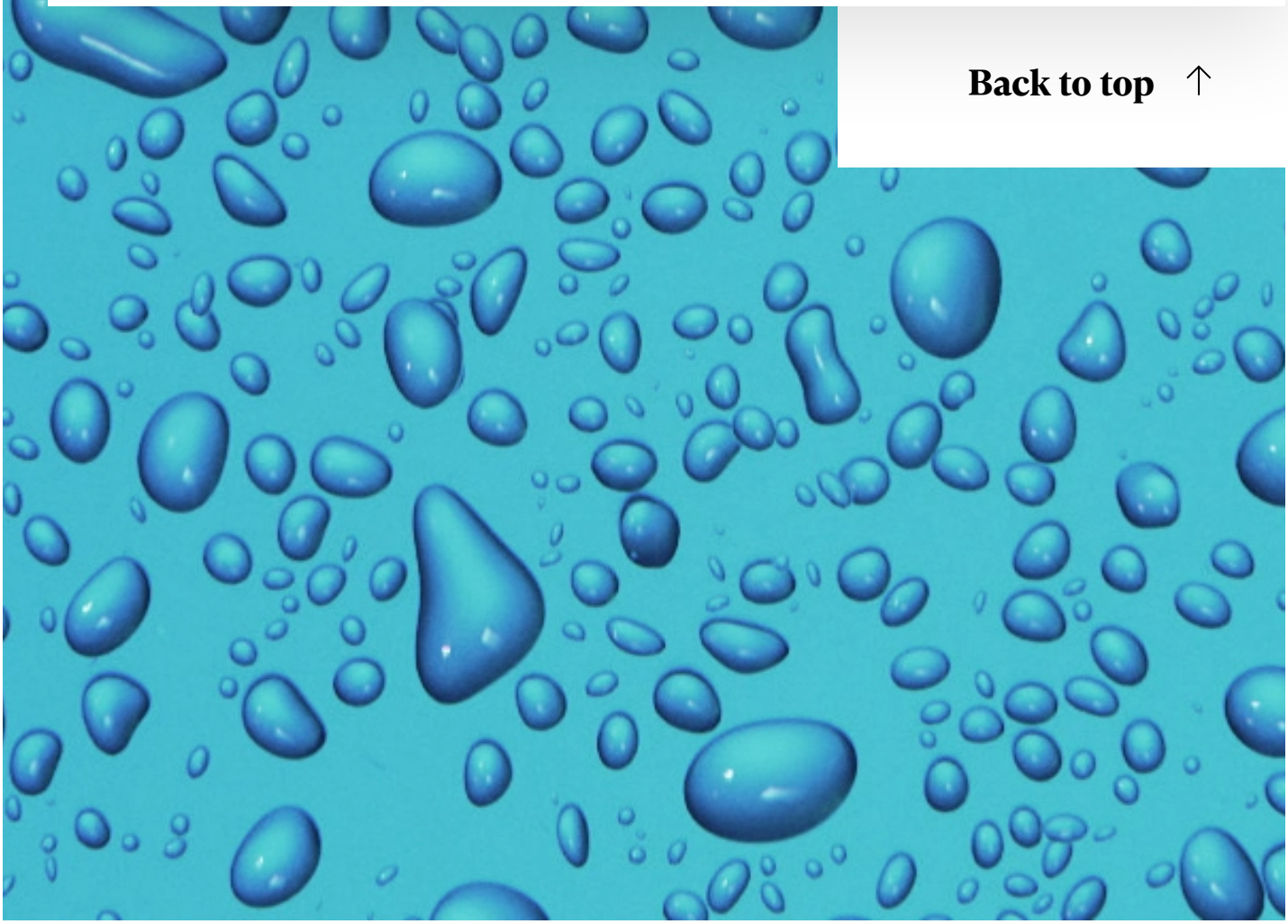
Inside the machine that saved Moore's Law

The Dutch firm ASML spent $9 billion and 17 years developing a way to keep making denser computer chips.

By Clive Thompson

Privacy Policy

Cover Art by Peter Crowther Associates



Back to top ↑